REMARKS/ARGUMENTS

The amended listing of claims and the following arguments are presented generally to impart precision to the claims, by particularly pointing out and distinctly claiming the subject matter. The pending claims are supported by the specification. No new matter is added.

Claims 2 and 8 were objected to for informalities. The current amendment removes the informalities.

Claims 1-6 and 20-22 were rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent No. 5,953,424 (hereinafter "Vogelesang"). Claims 24, 26-27 and 38-40 were rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of "Applied Cryptography" by Bruce Schneier (hereinafter "Schneier"). Claims 7-13, 17-19, 24, 26-32, 34-37 and 38-41 were rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of U.S. Patent Application Publication No. 2001/0042205 (hereinafter "Vanstone"). Claims 14-19, 25 and 33-37 were rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang in view of Vanstone and Schneier. Claim 23 was rejected under 35 U.S.C. 103(a) as being unpatentable over Vogelesang.

Applicant respectfully submits that the currently pending claims are patentable over the cited references.

Claim 1, for example, recites:

> 1. (Currently Amended) A cryptographic method, including:
>
> generating, at a first entity, a first session key K_B based on a second public key M_A;
>
> encrypting, at the first entity, a first random nonce N_B using at least a first password P_B and a first public key M_B to obtain an encrypted random nonce, the first public key M_B and the second public key M_A being session specific, the first public

key M_B to be used at a second entity to derive the first session key;

transmitting the encrypted random nonce from the first entity;

receiving a response to the encrypted random nonce; and

authenticating through determining whether the response includes a correct modification of the first random nonce.

In rejecting claim 1, the Office Action (e.g., Page 10, lines 1-8) took the following position.

1. "The second participant generates a session key using the second public key (Col 16, lines 41-42)" corresponds to "generating a first session key K_B based on the second public key M_A";
2. "The first participant ... encrypts the first random nonce with the session key which is a function of a password and a first public key, Y (Col 16, lines 64-67) corresponds to "encrypting the first random nonce N_B using at least a first password P_B and a first public key M_B to obtain an encrypted random nonce".

However, Vogelesang does not teach or suggest a same entity that performs both "generating a first session key K_B based on a second public key M_A" and "encrypting a first random nonce N_B using at least a first password P_B and a first public key M_B to obtain an encrypted random nonce, the first public key M_B and the second public key M_A being session specific, the first public key M_B to be used at a second entity to derive the first session key". In Vogelesang, ***different participants*** perform the operations that are relied upon for the rejection. Thus, Vogelesang does not anticipate claim 1.

For the reasons discussed above, Vogelesang does not anticipate independent claims 20-22. Therefore, the withdrawal of the rejections for claims 1, 20-22 and their dependent claims is respectfully requested.

Further, for example, claim 2 recites:

2. (Currently Amended) The method of claim 1 wherein said encrypting the first random nonce N_B includes:
generating a first secret S_B from at least the first password P_B and the first public key M_B; and
encrypting the first random nonce N_B using at least the first secret S_B;
wherein the first secret S_B and the first session key K_B are different.

Vogelesang does not show the generation a secret different from a session key.

In rejecting claims 7-10 and 29-31, the Office Action asserted that Vanstone describes:

> "The session key K, which is a function of first and second public keys (x and y), is combined with a^y which is a password to form a secure hash using a hashing algorithm (SHA-1)" (Page 7, lines 18-19, Office Action mailed July 14, 2005).

Applicant respectfully disagrees. In Vanstone, x and y are random integers generated at A and B respectively. Integers x and y are not transmitted as public keys.

Further, Vanstone does not show a secret that is different from the session key. Claim 2 recites "the first secret S_B and the first session key K_B are different" and "***encrypting*** the first random nonce N_B ***using at least the first secret*** S_B". Thus, even if Vogelesang and Vanstone were combined, the references do not show "***the first secret*** S_B" that is used to encrypt the random nonce.

Further, in Vanstone, the session key K and the value α^y are combined with a cryptographic function to generate the value h. The value h is sent to party A with the value α^y in the clear. Thus, the value h is not used to encrypt a random nonce. Thus, Vanstone and Vogelesang do not show "said generating the first secret S_B includes: ...; hashing the first result with a secure hash" (see, e.g., claim 8). In the Vanstone, the hashing operation is not part of "said generating the first secret S_B" which is used to "encrypting the first random nonce N_B" (see, e.g., claim 2).

In rejecting claims 24, 38-40, the Office Action asserted that Vanstone describes:

> "Vanstone discloses a similar cryptographic system in which a session key is generated based on first and second public keys (x and y) and a password such as a private key p_b" (Page 6, lines 24-26, Office Action mailed July 14, 2005).

Applicant respectfully disagrees. In Vanstone, x and y are random integers generated at A and B respectively. There is no indication in Vanstone that random integers x and y are transmitted as public keys for a specific session.

In rejecting claims 14-19, 25 and 33-37, the Office Action asserted that Vanstone describes:

> "Vogelesang in view of Vanstone disclose the construction of two separate session keys." (Page 9, line 6, Office Action mailed July 14, 2005).

Applicant respectfully disagrees. The Office Action failed to demonstrate why one would use two separate session keys in view of Vogelesang and Vanstone. Thus, the rejection for claims 14-19, 25 and 33-37 is improper.

Further, for example, claim 18 recites:

> 18. (Previously Presented) The method of claim 17 wherein said encrypting the modified second random nonce includes:
> generating a string of random bits I_B;
> encrypting a combination of the string of random bits I_B and the modified second random nonce using the first secret S_B to generate a first result; and

encrypting the first result using the first session key K_B.

In rejecting claim 18, the Office Action failed to find what in the references corresponding to the limitation of "a string of random bits I_B". Vogelesang does not have the further operation of "encrypting the modified second random nonce …", since the authentication process of Vogelesang ends when the correctness of M, as a response to the private signal L is verified. Furthermore, the references do not show "encrypting *a combination of the string of random bits I_B and the modified second random nonce* using the first secret S_B to generate a first result" and "encrypting the first result using the first session key K_B".

In another aspect, for example, claim 24 recites:

24. (Previously Presented) A cryptographic method, comprising:
receiving at a first entity a second public key M_A and an encrypted second random number;
generating a first session key K_B based on the second public key M_A;
decrypting, using at least a first password P_B and the second public key M_A, to retrieve a second random number N_A from the encrypted second random number;
modifying the second random number N_A to obtain a modified second random number;
encrypting the modified second random number using at least the first password P_B and a first public key M_B to obtain an encrypted random package; and
transmitting the encrypted random package from the first entity.

Applicant respectfully submits that a person skilled in the art would not reach a method as recited in claim 24 from the description of Vogelesang and Kaufman.

The Office Action asserted that "Kaufman describes an authentication similar to Vogelesang's in which a first entity, server, initially receives a password encrypted nonce." Applicant respectfully disagrees.

According to Kaufman (Col. 3, lines 51-59), the server receives a first argument and a second argument. The first argument of Kaufman is a password of the user. The password is encrypted using a first one-way cryptographic transformation function for the first argument. The second argument includes an encrypted version of a combination of an encrypted version of the password and a nonce. According to Kaufman (Col. 4, lines 14-18), the second argument includes the nonce to defeat the attempt of an eavesdropper to replay previously recorded arguments.

From this description of Kaufman, a person skilled in the art understands that Kaufman and Vogelesang have dramatically different methods for authentication. In Kaufman, the passwords of the users are transmitted over the network, in an encrypted form, for authentication. In Vogelesang, no password is transmitted for authentication. In Vogelesang, the secret information used for authentication (e.g., K and J) is not transmitted. The methods of Kaufman and Vogelesang are dramatically different. It is not apparent how the methods of Kaufman and Vogelesang might be combined and implemented with a reasonable expectable of success.

The Office Action asserted that "The password from a database is then used to obtain the random number." Applicant respectfully requests the examiner point out the particular description of either Kaufman or Vogelesang which supports such an assertion.

The Office Action relied upon Vogelesang (Col. 13, lines 41-67; Col. 14, lines 1-4) for a description of an authentication scheme which involves two nonces (L and V). However, applicant respectfully submits that Vogelesang describes the method of Col. 13, lines 41 – Col. 14, lines 4 to show the problems in this method. See, for example, Col. 14, lines 5-31. Thus, from the description of Vogelesang, a person skilled in the art understands that the method of Col. 13, lines 41 – Col. 14, lines 4 is a method separate from the method of Col. 16, lines 26 – Col. 17, lines 37. The method of Col. 16, lines 26 – Col. 17, lines 37 is proposed by Vogelesang to replace the method of Col. 13, lines 41 – Col. 14, lines 4, because of the problems as described in Col. 14, lines 5-31, Vogelesang.

Thus, applicant respectfully submits that it is improper to mix and match the elements of the method of Col. 13, lines 41 – Col. 14, lines 4 in Vogelesang with the method of Col. 16, lines 26 – Col. 17, lines 37 of Vogelesang. Here, one method is proposed to overcome the problems of another. It is not clearly why one would mix and match the methods.

Further, the combination of Vogelesang and Kaufman suggested in the Office Action is not proper. Kaufman does not show a random number encrypted by a password. Further, for the combination of Vogelesang and Kaufman suggested in the Office Action, the Office Action did not point out a complete consistent method, which might be implementation with reasonable expectable of success.

Furthermore, neither Vogelesang nor Kaufman suggests "decrypting, *using at least a first password P_B* ***and*** *the second public key M_A*, to retrieve a second random number N_A from the encrypted second random number" and "encrypting the modified second random number *using at least the first password P_B* ***and*** *a first public key M_B* to obtain an encrypted random package".

Thus, at least for the above reasons, claim 24 is patentable over Vogelesang and Kaufman.

Further, for example, claims 25 and 34 recite additional limitations not found in Vogelesang and Kaufman.

25. (Previously Presented) The method of claim 24, wherein said decrypting includes:

decrypting the encrypted second random number using the first session key K_B to generate a first decrypted result; and

decrypting the first decrypted result using at least the first password P_B and the second public key M_A.

34. (Previously Presented) The method of claim 24, further including:

generating a first random number N_B; and

wherein said encrypting the modified second random number includes:

encrypting a combination of the first random number N_B and the modified second random number.

The remaining claims depend from at least one of the claims discussed above, or recite similar limitations discussed above, and therefore include at least some of the distinguishing claim limitations as discussed above. As a result, the remaining claims are also patentable.

Authorization is hereby given to charge our Deposit Account No. 02-2666 for any charges that may be due or credit any overages. Furthermore, if a further extension is required, Applicant hereby requests such extension.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: 10/13, 2005

James C. Scheller, Jr.
Reg. No. 31,195

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025-1026
(408) 720-8300